REMARKS

Claims 17-19 have been added, and therefore claims 1 to 19 are now pending.

Reconsideration is respectfully requested based on the following.

Paragraph 12 of the Office Action concerns an objection to the wording of claim 1 for interchangeably using "programming unit" and "control unit." Claim 1 has been rewritten. Withdrawal of this objection is respectfully requested.

Paragraphs 13 and 14 of the Office Action concerns to an indefiniteness based on the language "encrypted in the control unit" of claim 1. It is respectfully submitted that the antecedent basis for the control unit is "a control unit" as found in the preamble of claim 1. Therefore, it is respectfully requested that this rejection be withdrawn.

With respect to paragraphs five (5) to ten (10) of the Office Action, it appears (but it is unclear) that the Office maintains the obviousness rejections of claims 1 to 4 and 6 to 16 under 35 U.S.C. § 103(a) as unpatentable over the Kawano reference in view of the Menezes reference.

In rejecting a claim under 35 U.S.C. § 103(a), the Examiner bears the initial burden of presenting a *prima facie* case of obviousness. In re Rijckaert, 9 F.3d 1531, 1532, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). To establish prima facie obviousness, three criteria must be satisfied. First, there must be some suggestion or motivation to modify or combine reference teachings. In re Fine, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988). This teaching or suggestion to make the claimed combination must be found in the prior art and not based on the application disclosure. In re Vaeck, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991). Second, there must be a reasonable expectation of success. In re Merck & Co., Inc., 800 F.2d 1091, 231 U.S.P.Q. 375 (Fed. Cir. 1986). Third, the prior art reference(s) must teach or suggest all of the claim features. In re Royka, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974).

The Office Action contends that a hash function alone performs the "no byte-wise allocation between input and output data occurs" function. The Office Action apparently indicates that when "no byte-wise allocation between input and output data occurs," this means that input strings are different lengths than output strings. Even if it were true that if output strings are different lengths than input strings, then no byte-wise allocation between input and output data has occurred, it is not true that if no byte-wise allocation has occurred, then input and output strings are necessarily of different lengths. Moreover, it is respectfully submitted that the Office Action reflects a misunderstanding of what is occurring during a hash function.

A hash function alone does not necessarily cause a lack of byte-wise allocation between input and output data. The hashing function creates an additional step in the decryption process so that additional security is provided. The hashing function creates a reference to an encryption key, but it does not cause the output data not to correspond to the input data, but rather causes the decryption device to reference the hash value to decode the key to be applied to the encrypted data, so that the key is not sent directly along the data line. In short, the hash function has no bearing on the string length.

It is irrelevant whether the Kawano reference operates on a complete stream of data, since it does not perform the "no byte-wise allocation between input and output data occurs" function. A hash function performed on a complete stream of data will allocate input and output data unless something additional is done. In the context of the claimed subject matter, a way to avoid byte-wise allocation is to rotate the input bits. (See Specification, p. 4 (describing the reversible operations of first a leftward rotation of bits within a byte by multiples of 8, after which encryption is performed on the resulting bits)). That is, no byte-wise allocation between input and output data occurs because the bits of an input do not correspond to the bits of an output (i.e., the encrypted byte does not correspond to the decrypted byte in the same position).

In contrast, if the Kawano reference apparently has byte-wise allocation between input and output data, it is because rotation does not occur. The Kawano reference refers to a hashing mechanism that encrypts data, but the resultant data nonetheless corresponds to the input data. The key that was applied to encrypt the input data, whether originating from a hashing function or not, does not charge the order of the output data as compared to the input data. Figures 11D and 11E of the Kawano reference refers to a hash value to be input into a hash table to determine the correct key for decrypting the encrypted data, but the encrypted data 72 corresponds one-to-one with the unencrypted data 71. This means that the "no byte-wise allocation" feature of the claimed subject matter is not met. But even if the "no byte-wise allocation" feature could be met, the "complete data stream" feature would not necessarily be met. In other words, the claimed subject matter is novel due to the increased security of a rotational step performed in the claimed invention.

In sum, independent claim 1 is allowable, as are its dependent claims.

In paragraph 16 of the Office Action, the Examiner rejected claims 1 to 16 under 25 U.S.C. 102(b) were rejected as anticipated by the Wasilewski reference.

As to claim 1, it is respectfully submitted that the Wasilewski reference does not identically disclose (or suggest) the feature in which "no allocation between input and output data occurs." The Office Action cites Wasilewski, col. 6, ll. 16-55, but this text only refers to using preferably a symmetric cipher, such as the DES algorithm. At no point does the Wasilewski reference introduce a new way of encrypting data, since it only pertains to a more large-scale system for encrypting cable service to cable consumers. As such, the Wasilewski reference does not identically disclose the particular low-level encryption mechanisms that are used. The output stream is allocated byte-wise in relation to the input stream. If it is not, that is because the complete stream has not been encrypted, so that some easily reversible re-ordering between encrypted and non-encrypted data portions has occurred in producing output data from input data. In any case, the references do not identically disclose (or suggest) the above-discussed features of the claimed subject matter, so that claim 1 is allowable, as are its dependent claims.

Claims 7 and 11 include features like those of claim 1 and are therefore allowable for the same reasons, as are their respective base claims. It is therefore respectfully submitted that claims 1 to 16 are allowable.

New claims 17 to 19 do not add any new matter and are supported in the specification. Claims 17, 18 and 19 respectively depend from claims 1, 7, and 11, and are therefore allowable for at least for the same reasons as their respective base claims.

It is therefore respectfully submitted that all of claims 1 to 19 are allowable.

Conclusion

In view of the foregoing, it is believed that the objections and rejections have been obviated, and that claims 1 to 19 are allowable. It is therefore respectfully requested that the objections and rejections be withdrawn, and that the present application issue as early as possible.

Respectfully submitted,
KENYON & KENYON LLP

Dated: 2/21/2007

By: GAMessina (By AD Reg. no. 33,865 Aaron C Deditch)
Gerard A. Messina
(Reg. No. 35,952)

One Broadway
New York, New York 10004
(212) 425-7200

CUSTOMER NO. 26646